UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	
	)	**CRIMINAL NO. 21-CR-30028-MGM**
BENJAMIN SHACAR,	)	
	)	
	)	
Defendant.	)	
	)	
	)	

DEFENDANT'S MOTION TO COMPEL DISCOVERY (REDACTED)

Now comes the defendant, Benjamin Shacar, who respectfully moves that the Court order the government to produce items of discovery pursuant to Local Rule 116.1 and Rule 16 of the Federal Rules of Criminal Procedure. The requested discovery is material to the preparation of Mr. Shacar's defense, necessary for the preparation and litigation of pretrial motions, and casts doubt on the admissibility of evidence in the government's case-in-chief. Mr. Shacar is therefore entitled to the discovery under Fed. R. Crim. P. 16(a)(1)(E), Local Rule 116, and *Brady v. Maryland*, 373 U.S. 83, 87 (1963). The requested items are as follows:

4. Any record of the investigative technique(s) utilized by the FLA with respect to the " notification" described in ¶32 in the affidavit in support of the search warrant submitted by Agent Yon.

5. Any and all cover sheet(s), correspondence, and/or index list documenting the totality of "tip" and/or "notification" information provided by the FLA described in ¶32 in the affidavit in support of the search warrant submitted by Agent Yon.

6. Complete copies of the "advisements" by the FLA to U.S. law enforcement regarding the "independent investigation" and "investigative work through which the FLA identified the IP address information" in this case, as referenced in ¶32 of the affidavit in support of the search warrant submitted by Agent Yon.

7. With respect to the notification by the FLA to U.S. law enforcement: please indicate whether, and how, the FLA determined that the defendant's IP address accessed and/or visited a

specific portion of the Target Website, and, if so, what specific portion of the Target Website was accessed and/or visited;

9. Any information, document, memorandum, and/or agreement addressing whether the FLA provided the information regarding the IP address in this case as part of a coordinated initiative or program with U.S. law enforcement.;

11. The name of the "Operation," "Task Force" "Initiative," and/or organizing group assigned by the FLA to the investigation in this case, and the name of "Operation," "Task Force," "Initiative," and/or organizing group assigned by the FBI to the investigation in this case, if different;

12. The specific case FBI ID and/or serial number assigned to the Defendant's case;

13. Any record of action taken in response to the FLA notification by U.S. Law Enforcement agencies, including but not limited to copies of subpoenas and supporting materials (including spreadsheets, charts, lists, and/or other documents) sent to internet service providers, as referenced in ¶41 of the affidavit in support of the search warrant submitted by Agent Yon of the affidavit; and copies of returns to such subpoenas.[1]

FACTUAL AND PROCEDURAL BACKGROUND

Mr. Shacar is charged, via indictment, with ten counts of receipt of child pornography in violation of in violation of 18 U.S.C. § 2252(a)(2)(A) and one count of one count of possession of child pornography in violation of 18 U.S.C. § 2252(a)(5)(B). The evidence against Mr. Shacar stems from materials discovered in his home pursuant to a search warrant. The allegations made in the search warrant affidavit and information omitted from that affidavit form the basis of the current dispute.

On March 22, 2021, Homeland Security Investigations ("HSI") Special Agent Daniel Yon applied for a search warrant to the U.S. District Court of Massachusetts. See Search Warrant Affidavit (attached as Ex. A filed under seal). Agent Yon sought authorization to search Mr. Shacar's home located in Pittsfield, Massachusetts for evidence, fruits, and instrumentalities of violations of 1) 18 U.S.C. §§ 2252(a)(1) and (b)(1) (Transportation of a Visual Depiction of a Minor Engaged in Sexually Explicit Conduct); 2) 18 U.S.C. §§ 2252A(a)(2) and (b)(1) (Receipt

[1] The numbers associated with these requests are taken from the Defendant's discovery letter dated August 28, 2023

or Distribution of a Visual Depiction of a Minor Engaged in Sexually Explicit Conduct); 3) 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (Possession of and Access with Intent to View a Visual Depiction of a Minor Engaged in Sexually Explicit Conduct); 4) 18 U.S.C. §§ 2252A(a)(1) and (b)(1) (Transportation of Child Pornography); 5) 18 U.S.C. §§ 2252A(a)(2) and (b)(1) (Receipt or Distribution of Child Pornography); and 5) 18 U.S.C. §§2252A(a)(5)(B) and (b)(2) (Possession of and Access with Intent to View Child Pornography). Ex. A at ¶ 4.

The affidavit submitted in support of the search warrant alleged that there was probable cause to believe that a user of the internet account at Mr. Shacar's home had accessed on a single date on May 2, 2019, a Tor hidden-services website geared towards the sexual exploitation of minors. Agent Yon did not specifically identify the target website in his affidavit. Specifically, Agent Yon stated:

> In August 2019, a foreign law enforcement agency (hereinafter, "FLA") known to U.S. law enforcement and with a history of providing reliable, accurate information in the past, notified U.S. law enforcement that the FLA had determined that on May 2, 2019, IP address 24.194.90.108 was used to access online child sexual abuse and exploitation material via a website that the FLA named and described as the TARGET WEBSITE.

Id. at ¶ 32. Agent Yon stated that the "FLA described the website facilitating 'the sharing of child sexual abuse and exploitation material stipulating only girls aged 5-13. Users were required to enter a username and password but these were only valid for that single login session' and provided further documentation naming the website as the TARGET WEBSITE, which the FLA referred to by its actual name." Id at ¶ 33.

Agent Yon also included a description of how the Tor network operates and how information is anonymized on the network, noting that "the Tor network attempts to [facilitate anonymous communication over the internet] by routing Tor user communications through a globally distributed network of intermediary computers, or relays, along a randomly assigned path known as a 'circuit.'" Id. at ¶ 9. Agent Yon acknowledged that because of this process, "traditional IP address-based identification techniques are not effective," but he neither expounded on the methodology used to identify the suspect user IP address in this case, nor provided any explanation for the reliability of the identification of the suspect user IP address. Id.

In the section of the affidavit discussing the FLA tips, Agent Yon claimed that the FLA (later identified by the government in response to defense discovery requests as the United

Kingdom's National Crime Agency) was a "national law enforcement agency of a country with an established rule of law." Id. at ¶ 34. Agent Yon averred that there was a "long history of U.S. law enforcement sharing criminal information with FLA and FLA sharing criminal investigation information with U.S. law enforcement." Id. Agent Yon also stated that the FLA "had obtained that [tip] information through independent investigation that was lawfully authorized in FLA's country pursuant to its national laws." Id. He further noted that the FLA had "advised U.S. law enforcement that FLA had not interfered with, accessed, search or seized any data from any computer in the United States in order to obtain that IP address information." Id. He stated that "U.S. law enforcement did not participate in the investigative work through which FLA identified the IP address." Id.

Finally, Agent Yon alleged that prior tips provided by the FLA had:

> (1) led to the identification and arrest of a U.S.-based child pornography producer and `hands-on offender, and the identification and rescue of multiple U.S. children subject to that offender's ongoing abuse; (2) led to the seizure of evidence of child pornography trafficking and possession; and (3) been determined through further investigation to be related to targets that U.S. law enforcement investigation had independently determined were associated with child pornography trafficking and possession.

Id. at ¶ 35.

According to the affidavit, in March 2020, U.S. law enforcement sent a subpoena to Charter Communications for subscriber information related to the suspect user IP address. Id. at ¶ 41. Charter Communications provided law enforcement with a physical address – [redacted] Pittsfield, MA 01201 associated with the IP address as well as the customer name – Benjamin Shacar. Id. Agent Yon stated that a search of a public records database and RMV records indicated that Benjamin Shacar lived at that address. Additional RMV records indicated that a car registered to Mr. Shacar and another car registered to both Mr. Shacar and his wife, [redacted], were registered to both subjects at the address listed above. Id. at ¶¶ 42-43. Agent Yon also noted that on December 10, 2020 and January 14, 2021, surveillance disclosed the vehicles at the premises referenced above. Id. at ¶¶ 44-45. Agent Yon also stated that representatives of Eversource Energy indicated that service was being provided to Benjamin Shacar at the same address and that a check with the United States Postal Service showed that Benjamin Shacar was receiving mail at that address. Id. at ¶¶ 46-47. Agent Yon included the fact that a check of open source information from the internet showed a Facebook page for Benjamin

Shacar which displays a profile picture of a man and woman together. The male depicted in the picture matches Mr. Shacar's RMV photograph, and the female matches Mrs. Shacar's RMV photograph. In addition a Facebook page for [redacted] depicts a photograph of a female matching [redacted] RMV photograph. Another photo on the Facebook page shows a photograph of a woman holding a young child outdoors, near a house matching the description of [redacted], as well as the subject premises. Id. at ¶¶ 48-49.

A warrant to search Mr. Shacar's home was issued on March 22, 2021. See Search Warrant (attached as Ex. B filed under seal). The warrant was executed on March 24, 2021. Based on the evidence discovered at Mr. Shacar's home, Mr. Shacar was arrested and a complaint was filed alleging a violation of 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography). Mr. Shacar was later indicted on ten counts of receipt of child pornography and one count of possession of child pornography.

Following his indictment, Mr. Shacar, through predecessor counsel, submitted detailed and itemized requests for discovery on March 21, 2022. See Exhibit C, Discovery Letter, 3/21/22. On April 4, 2022, the government provided some responsive materials and answers to the defendant's first discovery letter and declined to provide responses to several other requests. See Exhibit D filed under seal, Government Response, 4/4/22. Sometime after the government's April 4, 2022 response, the defendant, again through predecessor counsel, submitted a supplemental discovery letter to the government, requesting additional specific and detailed items of discovery. On October 31, 2022, in response to an inquiry from predecessor counsel, the government indicated that it had provided all relevant discovery in the case and did not intend to provide any additional discovery materials. See Exhibit E, Government Response 10/31/22. On August 28, 2023, the defendant, through undersigned counsel submitted a further detailed and itemized request for discovery. See Exhibit F filed under seal, Discovery Letter, 8/28/23. The government responded to that request on January 25, 2024 by referencing its previous submissions and declining to disclose any additional materials. See Exhibit G, Government Response 01/25/24.

Through the discovery process, the government has provided few details regarding the allegations made in the affidavit. Relevant to this motion, the government has identified the FLA that provided the tip notifying U.S. law enforcement that a particular IP "was used to access child sexual abuse material" as the [redacted] National Crime Agency See Exhibit H filed

under seal. The government also produced four pages of heavily redacted documents related to the tip. See Exhibit I filed under seal.

Since filing his discovery requests, the defendant has learned the warrant obtained by Agent Yon was a batch warrant. That is, warrants nearly identical to this one, with only the name of the suspect and other individualized information changed, were issued by the FBI throughout the country. (See Case Comparison, attached as Ex. J.) Agent Yon just filled in the blanks – name, home address, IP address, etc. The boilerplate warrant is believed to have been drafted by other FBI agents. Each of these warrants follow a strikingly similar pattern: the FBI claims to have learned from a FLA tip in August of 2019 that a certain IP address accessed a target website in April or May of 2019.

Also common to all the warrants is the omission that this information was only learned after a much broader, far-reaching investigation, involving several countries and going back years. Indeed, an FBI document demonstrates that the FBI opened its preliminary investigation in this matter in January 2017, more than two years before the IP addresses that had purportedly visited the target websites were identified by a foreign law enforcement agency and transmitted to the FBI. (See Exhibit K.) In an affidavit that arose from the same operation as this case, law enforcement described the investigation as "collaborative" between U.S. and foreign law enforcement. United States v. Thomas S. Clark, Case No. 2:21-MJ-00147-JLW (W.D. Wash., March 11, 2021) (Complaint) ("Clark Complaint") attached as Exhibit L, at ¶ 5. Press releases and the volume of information that the FBI obtained in reference to this investigation are additional evidence that this was a joint operation, where U.S. law enforcement were working hand in hand with foreign law enforcement agencies to share information, take over targeted websites, and identify visitors to target websites. See Exhibits M and N filed under seal.

Since filing his discovery requests with the government, the defendant has learned through information provided from similar cases in this and other jurisdictions, that the server hosting the target website was located in a country that is neither the United States nor the [redacted] and that [redacted] law enforcement seized the server in [redacted] See Exhibit N.

Mr. Shacar then filed a motion to compel, under seal, on March 4, 2024.

LEGAL STANDARDS

Fed. R. Crim. P. 16(a)(1)(E) requires the government, upon the defendant's request, to turn over any item within the government's possession, custody, or control that (i) is material to preparing the defense, (ii) the government intends to use in its case-in-chief, or (iii) was obtained from or belongs to the defendant. The First Circuit has noted that "materiality" requires "some indication that pretrial disclosure of the information sought would have enabled the defendant significantly to alter the quantum of proof in his favor." *United States v. Goris*, 876 F.3d 40, 45 (1st Cir. 2017) (emphasis added). A "significant alteration may take place in a myriad of ways, such as uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment or rebuttal." Id.

Local Rule 116 outlines the government's discovery responsibilities in more detail. Relevant to this motion, Local Rule 116.1 reaffirms that the government must fulfill its discovery obligations under Fed. R. Crim. P. 16(a)(1). Local Rule 116.2 goes further and requires the government to produce exculpatory evidence, which includes, but is not limited to information that "tends to (1) cast doubt on defendant's guilt as to any essential element in … the indictment … (2) cast doubt on the admissibility of evidence that the government anticipates using in its case in-chief, that might be subject to a motion to suppress or exclude … (3) cast doubt on the credibility or accuracy of any evidence that the government anticipates using in its case-in-chief." This rule implements *Brady v. Maryland*, 373 U.S. 83, 87 (1963), in which the Supreme Court held that the failure to disclose exculpatory evidence is a violation of due process.

In *Franks v. Delaware*, 438 U.S. 154, 155-56 (1978), the Supreme Court held that a defendant is entitled to a hearing to challenge the truthfulness of statements in a search warrant affidavit if he makes "a substantial preliminary showing" that the statements were "knowingly and intentionally [false], or made with reckless disregard for the truth," and that the falsehood was "necessary to the finding of probable cause." Some courts have indicated that the same standard is required in order to obtain discovery to mount a *Franks* challenge. See, e.g., *United States v. Long*, 774 F.3d 653, 661-62 (10th Cir. 2014) (where defendant sought disclosure of the name and contact information of a confidential informant in order "to obtain evidence for a Franks hearing," the Court upheld denied of that request because the defendant "did not make an adequate evidentiary showing under *Franks*").

However, at least one court in this district has acknowledged the difficult, if not impossible, burden that rests with the defendant when the *Franks* discovery sought relates to a confidential source. See *United States v. Jordan*, No. 09-10139-JLT, 2010 WL 625280, at *3 (D. Mass. Feb.23, 2010) ("the courts recognize that when an affidavit relies primarily on information provided by a [confidential informant], a defendant will lack the information needed to make a Franks showing.") (citing *United States v. Manning*, 79 F.3d 212, 220 (1st Cir. 1996)). That court held –in the context of a defendant who sought information about a confidential informant – that the production of discovery related to a Franks challenge "should await an initial showing, at a minimum, that there are inaccuracies in the affidavit and that if the challenged information is omitted, there is no probable cause for the warrant." *Jordan,* 2010 WL 625280, at *4.

ARGUMENT

The requested items outlined below are discoverable under Rule 16(a)(1)(E) because: (1) Mr. Shacar has requested them, (2) the items are in the Government's possession, custody, or control, and (3) the items are material to the preparation of Mr. Shacar's defense. See Fed. R. Crim. P. 16(a)(1)(E). The information sought by Mr. Shacar is exculpatory, as it casts doubt on the accuracy of the information in the search warrant and therefore goes directly to the "admissibility of evidence the government anticipates offering in its case-in-chief." Local Rule 116.2(a); *Brady*, 373 U.S. at 87. The materials available to Mr. Shacar suggest that there was, at minimum, a collaboration between the United States and the FLAs in the investigation in this case.

Generally, the Fourth Amendment's exclusionary rule does not apply to foreign searches and seizures." United States v. *Valdivia*, 680 F.3d 33, 51 (1st Cir. 2012). There are, however, two exceptions to that rule: "(1) where the conduct of foreign police shocks the judicial conscience, or (2) where American agents participated in the foreign search, or the foreign officers acted as agents for their American counterparts. Mr. Shacar is entitled to discovery that further reveals the level of collaboration between the United States and the FLAs because it goes to the heart of whether the FLAs' investigations involved searches within U.S. territory, and whether the FLAs acted with U.S. agents, at the behest of U.S. agents, or as agents for their American counterparts, such that there was a "joint venture" or that it constituted activities which would shock the conscience in violation of the Fourth Amendment. The requested discovery must also be turned over because Mr. Shacar has made an initial showing

that there are inaccuracies in the affidavit and that if those inaccuracies are corrected, and if omitted information is added to the affidavit, probable cause to search Mr. Shacar's home is absent. *Franks*, 438 U.S. at 155-56. This initial showing entitles Mr. Shacar to further discovery that is material to a *Franks* motion and his motion to suppress.

Discovery Request #5. *Any and all cover sheet(s), correspondence, and/or index list documenting the totality of "tip" and/or "notification" information provided by the FLA described in ¶ 32 in the affidavit in support of the search warrant submitted by Agent Yon.*

Discovery Request #6. *Complete copies of the "advisements" by the FLA to U.S. law enforcement regarding the "independent investigation" and "investigative work through which the FLA identified the IP address information" in this case, as referenced in ¶ 32 of the affidavit in support of the search warrant submitted by Agent Yon.*

With respect to item #5, the defense has received a seemingly incomplete set of heavily redacted documents. The first document contains an undated single-page report that alleges an IP address was once "used to access online child sexual abuse and exploitation material" on May 2, 2019. See Exhibit H filed under seal. The second document is a single letter from the [redacted] National Crime Agency to the FBI – addressed to an unnamed person/unit within the FBI, and authored by an unnamed person/unit in the [redacted] National Crime Agency that does not reference the single page report by either date or reference number or reference the IP address named in the report. Exhibit O filed under seal.

These documents are not only not responsive to Mr. Shacar's request but also suggest that more documentation exists and has been withheld. Agent Yon's affidavit specifically states that the FLA – now identified as the [redacted] National Crime Agency – "notified U.S. law enforcement that the FLA had determined that on May 2, 2019… [the IP address] was used to access online child sexual abuse and exploitation material via a website that the FLA named and described as the TARGET WEBSITE. Exhibit A at ¶ 32. The affidavit also refers to other "documentation naming the TARGET WEBSITE." Exhibit A at ¶ 33. None of the documents provided so far have connected the website by name with the specific IP address and the specific date mentioned in the affidavit.

In the event that the government argues that the defendant has not made a substantial showing to obtain discovery prior to a Franks hearing, the defendant contends that the previously cited *Jordan* case from this district suggests that the defendant does not need to make a

"substantial" showing to obtain discovery prior to a Franks hearing. In *Jordan*, 2010 WL 625280, at *3-4, and that the production of the discovery sought should await an "initial showing" of inaccuracies in the affidavit that, if omitted, would preclude a probable cause finding.

Under either standard, Mr. Shacar has sufficiently shown that there are material inaccuracies and omissions in the affidavit. Principally, Agent Yon misrepresented the nature and origin of the tip from [redacted] National Crime Agency. In the affidavit, Agent Yon stated that U.S. law enforcement was notified by an FLA that a specific IP address had accessed child sexual abuse material on May 2, 2019 Exhibit A at ¶ 32. From the documents provided to the defense, it is clear that Agent Yon's statement in the affidavit is inaccurate. Rather than repeating the tip verbatim, Agent Yon added language and omitted information to make it appear to the Magistrate that U.S. law enforcement had more evidence of criminal activity than it actually did. For example, Agent Yon omitted from the affidavit the now-apparent fact that U.S. law enforcement had no evidence that an internet user associated with that IP address had created an account the website or logged into the website. Agent Yon also omitted from the affidavit the fact that U.S. law enforcement had no evidence of what, if anything, was actually "accessed", viewed, or downloaded on that date at that time.

Agent Yon also made a number of misrepresentations regarding the reliability of the tip. In the affidavit, Agent Yon stated that the FLA that provided the tip ([redacted] National Crime Agency) was a "national law enforcement agency of a country with an established rule of law." Exhibit A at ¶ 34. Agent Yon further stated that the FLA advised U.S. law enforcement that it "had not interfered with, accessed, searched, or seized any data from any computer in the United States in order to obtain that IP address information." Id. Finally, Agent Yon claimed that prior tips from the FLA had led to 1) the identification and arrest of a U.S.-based child pornography producer and hands-on offender, and the identification and rescue of multiple U.S. children subject to that offender's ongoing abuse; 2) to the seizure of evidence of child pornography trafficking and possession; and 3) been determined through further investigation to be related to targets that U.S. law enforcement investigation had independently determined were associated with child pornography trafficking and possession. Exhibit A at ¶ 35.

However, Agent Yon failed to include the fact that there was not just one FLA involved in obtaining the IP address, but two – from two different countries – and thus that the

government's representations and assurances in the affidavit about either the scope of U.S. involvement or the denial of interaction with any computer in the U.S. applied only to the FLA that provided the tip to U.S. law enforcement (again, the [redacted] National Crime Agency) Agent Yon did not make this distinction in the affidavit, and instead created the impression that the tip and the source of that tip both originated from the same, reliable FLA. This impression was misleading and inaccurate. Notably, the government has made no similar such assurances or representations about the lack of U.S. involvement in the seizure of the server, or the absence of coordination or collaboration with the seizing FLA. Neither has the government made any similar such assurances or representations about the deployment of investigative techniques by the seizing FLA, with or without U.S. involvement, to interfere with, access, search, or seize any data from any computer in the U.S.

These inaccuracies about the nature and reliability of the tip go to the heart of the probable cause analysis. The tip from the FLA was the only allegation of criminal activity in the entire affidavit. It was also the only piece of information that created any nexus to Mr. Shacar and his home. If these inaccuracies were corrected, and if the omitted information were added, the affidavit would not establish probable cause to search Mr. Shacar's home. This "initial showing" is sufficient to warrant further discovery prior to a Franks hearing.

Discovery Request # 4 *Any record of the investigative technique(s) utilized by the FLA with respect to the "notification" described in in ¶ 32 in the affidavit in support of the search warrant submitted by Agent Yon.*

The government refuses to provide any information regarding the investigative technique utilized by the [redacted] National Crime Agency or [redacted] Law Enforcement to identify the IP address in this case, and the investigative technique, if different, to link the IP address to the target websites. However, the manner in which the IP address was identified and de-anonymized – whether it was through the use or deployment of a network investigative technique ("NIT"), or some other means – is material because it is crucial to determining whether a search occurred.

An expert declaration submitted in a case virtually identical to Mr. Shacar's suggests that the specific IP address could not have been identified without running a NIT or, in the alternative, an error-prone traffic analysis technique. See Declaration of Steven Murdoch at ¶ 22-32, United States v. Sanders, No. 20-cr-00143 (E.D. Va. Sept. 17, 2021), ECF No. 464-2,

attached as Exhibit P. Either scenario would significantly undermine the veracity of the affidavit and its probable cause showing. The deployment of a NIT would constitute an unlawful warrantless search, the results of which could not be considered in Agent Yon's affidavit. See e.g., *United States v. Anzalone*, 208 F. Supp. 3d 358, 366 (D. Mass. 2016). The use of a NIT would also reveal a substantial misrepresentation in the affidavit, which relies on Agent Yon's assurance that no computer in the United States had been searched. Exhibit A at ¶ 34. Alternatively, the fact that the traffic analysis technique described in Professor Murdoch's declaration is inherently error-prone would undermine the strength and reliability of the tip such that no magistrate, had he or she been aware that this technique was used to obtain the IP address, would find there was probable cause. See Exhibit P at ¶ 22-32.

The technique used to identify the IP address is also material to whether, and to what extent, U.S. law enforcement directed, assisted, and/or participated in the investigation as outlined in Discovery Requests #6. In the affidavit, Agent Yon claimed that U.S. law enforcement had not participated in the investigative work "through which FLA identified the IP address information provided by FLA." Exhibit A at ¶ 34. However, as argued above, Agent Yon deliberately obscured the fact that there were two distinct FLAs, from two different countries, involved in obtaining the IP address. The Agent's assurances that U.S. law enforcement did not "participate" only applied to the [redacted] National Crime Agency not [redacted] Law Enforcement, which actually seized the server. The government has made no such assurances as to that FLA.

Discovery Request # 9 *Any information, document, memorandum, and/or agreement addressing whether the FLA provided the information regarding the IP address in this case as part of a coordinated initiative or program with U.S. law enforcement*

The government's response to this discovery request did not address whether the U.S. was involved in any investigative phase of this operation, whether the U.S. provided or requested information during the course of the operation, or whether it was conducted pursuant to an understanding, memorandum, collaboration, cooperation, mutual assistance treaty, and/or agreement between U.S. law enforcement and the FLA, or at the behest, direction, and/or benefit of the U.S. The requested discovery is material and potentially exculpatory. The requested material relates to the existence of a joint venture between the United States and the FLAs, which is central to the Fourth Amendment issues in this case.

Critically, information gleaned as a result of FOIA requests show that prosecutors in the U.S. Attorney's Office in Massachusetts were working on an affidavit in support of a search warrant before the government claims to have received the lucky tip. In emails in July of 2019 – months before the "tip" in either August or November of 20191 – agents and attorneys at the U.S. Attorney's office for the District of Massachusetts ("USAMA"), were sending emails to each other with the subject line "affidavit so far." (attached as Exhibit Q, highlighting added). Later, the subject line is changed to "Tor OP go by." (Id.) Further emails were sent in September of 2019 discussing "website A" and "B." (Id.) Other emails contains an attachment entitled "[Country 1]2 storage devices affidavit." (Id.) These emails, in short, contain attachments for residential search warrants in the United States before the government claimed to have known of any U.S.-based IP addresses associated with the site. It is devastating to the claim that the U.S. government received a tip and only then began seeking out U.S. IP addresses associated with the site. They were drafting warrants and including descriptions of the websites before the "tip" was even received.

> ***Discovery Request #10****: Complete copies of the "advisements" by the FLA to U.S. law enforcement regarding the "independent investigation" and "investigative work through which the FLA identified the IP address information" in this case, as referenced in ¶ 32 of the affidavit.*

Mr. Shacar is entitled to the requested discovery for the same reasons outlined in Discovery Requests #4

> ***Discovery Request #11***: *The name of the "Operation," "Task Force," "Initiative," and/or organizing group assigned by the FLA to the investigation in this case, and the name of "Operation," "Task Force," "Initiative," and/or organizing group assigned by the FBI to the investigation in this case, if different.*

> ***Discovery Request #12***: *The specific case FBI ID and/or serial number assigned to the Defendant's case.*

These discovery requests relate to the scope of the operation, the nature of any joint investigation and/or coordinated steps taken by different law enforcement agencies, and the membership(s) and/or role(s) of various law enforcement agencies and actors. As further investigation now reveals, more than one FLA was involved in the investigation and the roles of the FBI and the FLA's remain unclear.

The report from [redacted] National Crime Agency in this case appears to be one of many reports that are part of an as-yet unnamed operation that resulted in the identification of multiple IP addresses at the same time. Defense counsel has reason to believe that the name of this overarching operation has been disclosed in other cases similar to Mr. Shacar's. Although those cases are subject to restrictive protective orders, the facts that are available are strikingly similar to those in Mr. Shacar's. See Exhibit J. The name of the operation and the case number assigned to Mr. Shacar's case are relevant to the scope of this operation and are, for the reasons outlined above, material and exculpatory.

Discovery Request #13. *Any record of action taken in response to the FLA notification by U.S. Law Enforcement agencies, including but not limited to copies of subpoenas and supporting materials (including spreadsheets, charts, lists, and/or other documents) sent to internet service providers, as referenced in ¶ 41 of the affidavit in support of the search warrant submitted by Agent Yon of the affidavit; and copies of returns to such subpoenas.*

The government responded to this request as follows: "The Government provided information responsive to this request on June 3, 2021 and March 3, 2022. The Government will supplement its response to this request by posting a "preservation letter" sent to Google, Inc., onto USAFx by January 26, 2024." See Exhibit G.

The undersigned counsel was not counsel of record for Mr. Shacar on the dates specified by the government in its response to this request. Counsel retrieved the file of predecessor counsel when appointed to Mr. Shacar in March, 2023. A review of the file received from predecessor counsel fails to show any documentation which appears to be responsive to this request. In paragraph 41 of Agent's Yon's affidavit in support of search warrant, he describes the issuance of a subpoena/summons to Charter Communications and results from said issuance. This information may have been given to predecessor counsel, but the undersigned does not have this information. The request is relevant as the defendant seeks to confirm the accuracy of the information contained in Agent's Yon's affidavit.

Discovery Request # 7 *With respect to the notification by the FLA to U.S. law enforcement: please indicate whether, and how, the FLA determined that the defendant's IP address accessed and/or visited a specific. portion of the Target Website, and, if section, what specific n of the Target Website was accessed and/or visited.*

The government's response was "The affidavit in support of the search warrant application in this matter describes how the FLA provided the information leading to your client's IP address, the description of the target website, and the context of the FLA has provided information in the past. Also, see response to request 4." Exhibit G. This response is not responsive to the defendant's request as Agent Yon's affidavit simply indicates that the IP address associated with the defendant "was used to access online child sexual abuse and exploitation material" via the target website. See Exhibit A, ¶ 32. The government has failed to disclose the technique used by the FLA's to identify the IP address that accessed the websites. The government must produce that information for the same reasons outlined in Discovery Request #8. Additionally, the government's assertion does not relieve it of its constitutional obligations under *Brady* to disclose exculpatory evidence. See also *Kyles v. Whitley*, 514 U.S. at 437.

CONCLUSION

For the above stated reasons, Mr. Shacar respectfully requests that this Honorable Court allow the motion to compel discovery.

Respectfully submitted,

BENJAMIN SHACAR

/s/ William J. O'Neil

WILLIAM J. O'NEIL
Attorney for the Defendant
280 N. Main St., Ste. 6
East Longmeadow, MA 01028
(413) 224-2694
BBO#:548445

CERTIFICATE OF SERVICE

I hereby certify that true copies of this document will be served on the registered parties through the ECF system on this date March 4, 2024.

/s/ William J. O'Neil
William J. O'Neil
280 N. Main Street, Ste. 6
E. Longmeadow, MA 01028
(413) 224-2694
BBO#: 548445